Biometric User Authentication & System Security

Dr. Stephen Kent

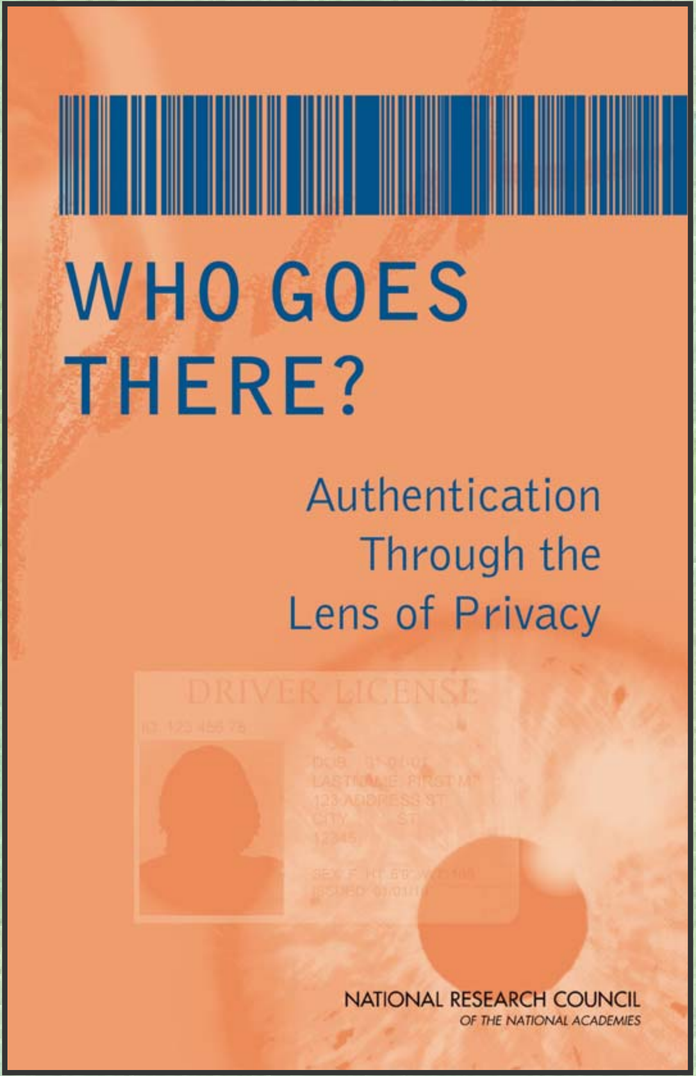
Chief Scientist - Information Security

BBN
TECHNOLOGIES

Today’s Topic

- Workshop charter
  - The objective of this workshop is to determine how biometrics can be used for remote e-authentication over open networks by providing equivalent authentication assurance to the conventional secret-based mechanisms defined in NIST Special Publication 800-63, for each of four authentication levels.
- My position
  - Maybe this is a bad idea
  - That was the conclusion of an NRC study committee

The NRC Report


WHO GOES THERE?
Authentication Through the Lens of Privacy
DRIVER LICENSE
NATIONAL RESEARCH COUNCIL
OF THE NATIONAL ACADEMIES

Prepared by:

Committee on Authentication Technologies and Their Privacy Implications

Computer Science and Telecommunications Board

The National Academies
Washington, D.C.
http://cstb.org/

Obtain a hardcopy of the report from: http://www.nap.edu

Biometrics & Authentication

- Confidentiality
- Access control
- Integrity
- Non-repudiation
- Authentication
  - **Initial (one way) authentication**
    - Identifying a principal at the beginning of a session
  - Two-way authentication
    - Identifying the entity at each end (e.g., client & server)
  - Continuous authentication
    - Maintaining the binding between session traffic and the identities authenticated during session initiation

Biometric Authentication Model

- Initial registration (usually ”face to face”)
  - User identification
  - Feature capture
  - Template construction
- User authentication (may be local or remote)
  - Identity assertion
  - Feature capture
  - Scoring against registration template

Biometrics in Different Contexts

- Authentication to a PC
  - Usually one user, maybe a few
  - Local registration and template storage (on the PC itself, maybe in a local server)
- Authentication to a smart card
  - Very local storage, just one user, goal is logically unlocking (not decrypting) cryptographic key
- Authentication to a server
  - Typically many users, remote storage of templates
- Interpersonal authentication
  - Generally not feasible, e.g., e-mail sender authentication

Are Biometrics Better than Secrets?

- Typical vendor claims
  - More secure
  - Less expensive
  - More convenient
- But, relative to what alternative user authentication technology?
  - Static passwords
  - One-time passwords
  - Challenge-response systems
  - Smart cards
  - Cryptographic systems (Kerberos, PKI)

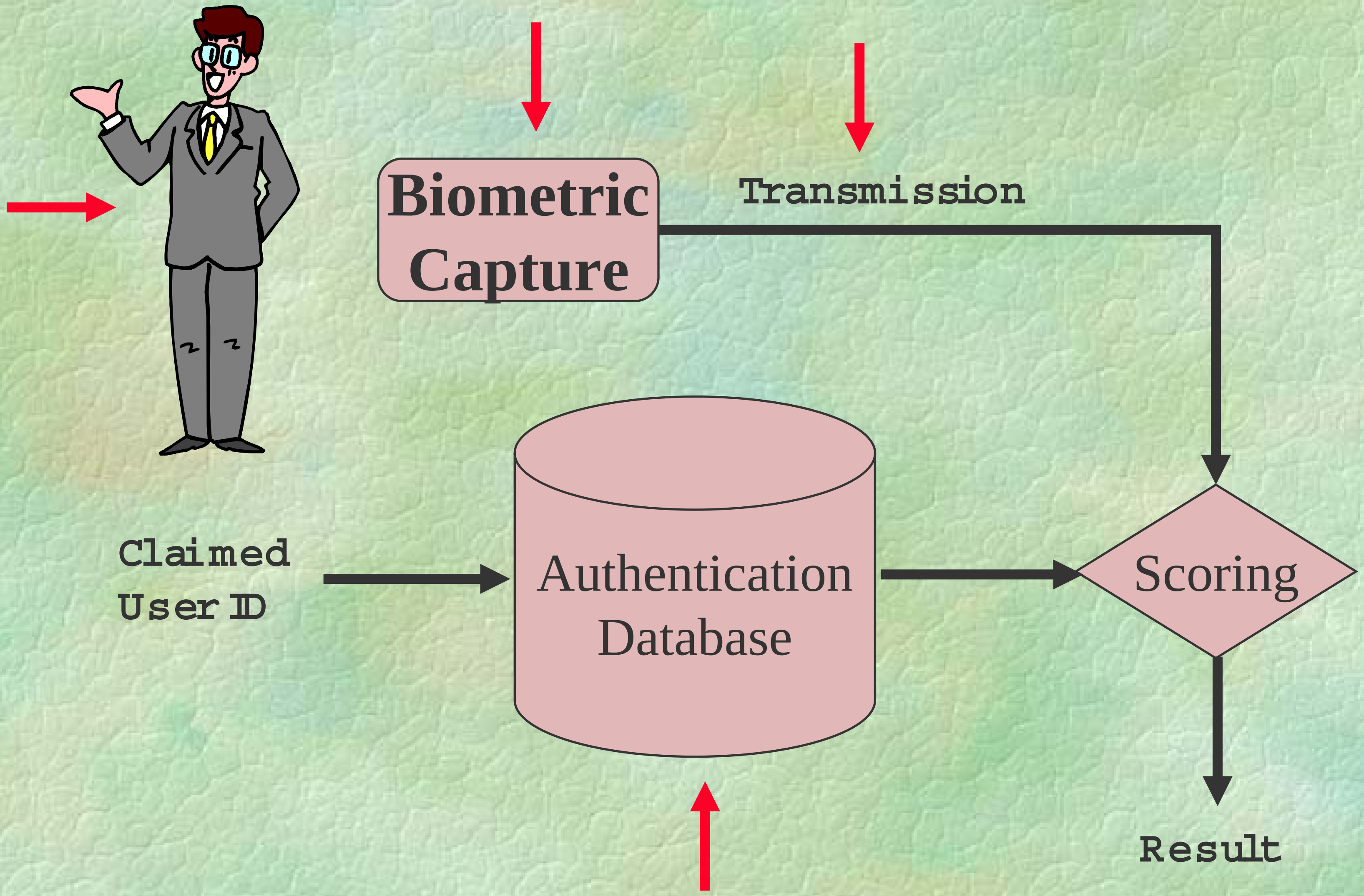
Truth in Advertising

- Biometric authentication can be much more convenient: nothing to remember, nothing to lose
- Capital costs are higher for biometric authentication, but life cycle costs could be lower, if not combined with a PIN/password
- But, typical systems using biometrics emphasize multi-factor authentication, excluding this possible benefit!

Are Biometrics More Secure?

- The security of biometric authentication must be evaluated relative to a perceived threat:
  - who are the adversaries?
  - what are their goals?
  - what are their capabilities?
- All biometric systems are imperfect, most have DET curves that are not very impressive, so as we tune to make systems “user friendly” we increase false positive %

Attack Points



Attacking Biometric Systems

- Fooling biometric sensors with fake body parts
- Using real body parts acquired from a user (e.g., in a non-cooperative fashion)
- Intercepting digitized biometric samples (transmission, compromised capture devices, …)
- Covert acquisition of biometric values from users
- Injecting purported biometric bit patterns into compromised capture devices
- Unauthorized acquisition of templates from authentication system components

Biometrics & Security

- Many computer/network authentication applications ultimately require crypto secrets
- Some biometric features are easily acquired and may be used to create bogus inputs to capture devices
- Most biometric capture devices used with PCs are vulnerable to many types of attacks, do not meet FIPS 140-2 criteria, …
- Authentication servers tend to store templates in a "recoverable" form that could be stolen
- We cannot change our biometric features as easily as we change passwords, PINs, or keys

A Worst Case Scenario

- A standardized biometric authentication technology is adopted on a widespread basis
- Biometric templates are stored on many servers
- Attackers break into one or more servers, stealing biometric templates
- Knowing the algorithms used and possessing user templates, attackers generate samples that mimic sample captures for these users (offline guessing)
- Attackers insert fake samples wherever capture system technology is not well protected

Good, Local Uses of Biometrics

- Authentication of a user to his/her PC
  - Used as the only factor in a home context where security is less important than convenience
  - Used with an additional factor in higher security contexts, as a means to counter password or physical token sharing
- Authentication of a user to a crypto token
  - To unlock a key, perhaps with a password/PIN
- Authentication of a user for physical access control in a physically well-protected context
  - Where tampering with the capture device is not likely

Workshop Questions

- 1. How can Federal agencies and other organizations use biometrics to authenticate unsupervised remote claimants whose computers and workstations they do not manage or control?
- 2. How do we compare the authentication assurance provided by unsupervised biometric methods to the conventional methods now defined in NIST Special Publication 800-63 ?
- 3. In what way could biometrics be appropriately used for each of the four authentication levels?
- 4. What constraints and protections need to be in place to use biometrics in a secure solution?

Answers?

- This may be an example of the worst possible case
  - No guarantee that transmitted bits represent a biometric
  - System relies on a giant database of templates, a juicy target!
- Biometrics used here are less flexible than secret-based mechanisms, e.g., can’t be used to sign a form or e-mail, which seems to limit secure user interaction options
- Use of biometrics don’t align with existing protocol standards for user authentication (e.g., SSL/TLS)
- Assurance seems less than level 4, maybe less than level 3
- Privacy concerns are MUCH greater that for any secret-based authentication mechanism

Conclusions

- Biometric user authentication technology can be convenient, may be cost effective, and can provide a secure basis for local authentication
- Cryptographic technology, e.g., PKI or Kerberos, usually is preferable for remote authentication
- Credible scenarios exist that could result in large scale exposure of user biometric templates and enable widespread spoofing of user identity
- Re the workshop questions, maybe Nancy Reagan’s famous words are appropriate:

  “Just Say No”

Faith-based User Authentication?

“User name and password?”